REMARKS

Summary

Claims 1, 5-6, 8, 11, and 19-33 remain pending in the application. No new matter was added.

Specification

The specification has been amended to correct an obvious typographical error in which the labels 201 and 202 were inadvertently switched in the text. This sentence now comports with the remainder of the specification.

Rejection of Claims under 35 U.S.C. §101

Claims 1, 5-6, 8, 11, and 19-33 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. The Office Action states that the claims are neither tied to another statutory class (such as a particular apparatus) nor transform underlying subject matter (such as an article or materials) to a different state or thing. In addition, the Office Action states that the tie to the statutory class cannot be an extra-solution activity but is extra-solution activity in the case of the instant claims. Applicant traverses the rejection.

Despite the previous response citing case law that is applicable and must be followed by the Patent Office, this rejection remains. Applicant urges the Examiner to review this law as the claims recite a number of limitations that make a 35 U.S.C. §101 rejection unwarranted. It is readily apparent that the steps recited by the recited methods cannot be carried out in abstract – they must be carried out by specific machines (e.g., reading by a scanner or other similar electronic apparatus as well as other electronic components). Per the cited case law and other CAFC and BPAI decisions it is unnecessary to recite the specific devices to accomplish the method steps – it is sufficient that they must be performed by specific machines.

Moreover, the claims recite at least some steps that are both transformative and necessary to determine if an item is fraudulent. Taking claim 1 for example, the state of the decision maker is transformed depending on the contents of the storage media. Furthermore, the Office Action is invited to explain how one can achieve the recited method without electronically/optically reading or otherwise obtaining both sets of contents, encrypting one of the sets of contents or performing the ensuing cryptographic decision-making process.

It is clear from Bilski that 35 U.S.C. §101 rejections should not be used unless the subject matter simply cannot be placed into a statutory class. The recited claims, on the other hand, at a minimum satisfy the "machine or transformation" test and thus do not fall into the category of claims that would run afoul of 35 U.S.C. §101.

For similar reasons as above, the rejection of claims 6, 11 and 21 based on 35 U.S.C. §101 is thus traversed.

If the Examiner insists on continuing this rejection in the next Office Action he is respectfully requested to contact Applicant's agent in an effort to avoid an extended discussion on this subject.

Rejection of Claims under 35 U.S.C. §112, first paragraph

Claims 30-33 were rejected under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement. Applicant traverses the rejection.

Claim 30 recites that (from claims 1 and 29, from which claim 30 depends) the RFID tag contains several numbers: a first number that contains a third number and a fourth number in which the third number is concatenated with, and contains different information than the fourth number. Specifically, the third number includes product information of the item while the fourth number does not.

The Examiner states that there is no support for these claims in the specification. However, among others as described in the second paragraph of the detailed description (and further discussed in the enumerated list thereafter) and in relation to step 501 of Fig. 5, the first number 201 (as recited fourth number) is a unique or semi-unique unalterable number existing on the anti-forgery RFID tag. This unique or semi-unique unalterable number is either obtained by the manufacturer from a semiconductor company or can be established by the manufacturer using a unique characteristic of the item's manufactured material (e.g., a unique painted pattern read using a laser to determine the unalterable number or a unique number impregnated in the material then read by a laser type device to determine the random number).

Thus, it is clear that while the third number 202 contains product information, the fourth number 201 does not contain product information (defined as manufacturer code, product code, serial number, etc… in the instant specification).

Accordingly, Applicant traverses the rejection and submits that the arguments are neither without merit nor is the invention lacking support in the specification and based entirely on new matter.

Rejection of Claims under 35 U.S.C. § 103(a)

Claims 1, 5-6, 8, 11, 19-25, 27-28 and 31-33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kay et al. (U.S. Patent 6,223,166; "Kay") in view of Halperin et al. (U.S. Patent 6,226,619; "Halperin"). Claims 26 and 29-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kay and Halperin in view of Coppersmith et al., (U.S. Patent 6,069,955; "Coppersmith"). Applicant traverses the rejection.

Claim 1 recites a method for determining if an item is fraudulent. The method comprises, *inter alia*, that a public-key cryptographic process is used to decide whether a number printed on the item/packaging is a public-key signature of a number in an RFID tag associated with the item/packaging. The authenticity of the item is then determined as a result of this decision. In other words, if the printed number matches the public-key signature of the RFID number, the authenticity is confirmed. Thus, it is clear that the public-key cryptographic process operates on the RFID contents and the printed number to determine if the printed number is a signature of the RFID contents.

Kay discloses a method of creating a printed ticket to an event, such as a sporting event or concert. The event information is generated and optionally signed. This information is encrypted and then printed as a ticket (e.g., as a bar code or label) by a customer. The customer takes the printed ticket to the event, where the ticket is read by a reader (portable terminal 27) held by an event official. The information in the ticket is decrypted by the portable terminal and the signature, if present, is verified. The decrypted information is compared with the event information stored in the memory of the portable terminal and if the event information on the ticket matches the event information, the portable terminal authenticates the ticket.

Claim 1 recites the use of first and second numbers that are related to a particular item and obtained by different means. The Office Action refers repeatedly to col. 4, lines 40-60 of Kay for the first and second numbers. It is clear, however, that Kay is directed to an event rather

than an item. Assuming, *arguendo*, that the ticket of Kay is considered an "item," Kay discloses only a single number -- the printed number on the ticket obtained by optically scanning the number. Kay does not disclose obtaining a different number associated with the ticket by radio means.

Consequently, nor does col. 4, lines 15-25 of Kay disclose using a cryptographic process to decide whether the second number is a signature of the first number, as indicated in the Office Action. In fact, the passage referred to in the Office Action only states generally that if the printed information contains an encrypted signature, two keys would be required to access the information and validate the ticket. This is, of course, well known and has nothing to do with using a cryptographic process to decide whether a first item number that is electronically read is a signature of a second printed number obtained by radio means.

Once again, the Office Action refers to col. 4, lines 40-60 of Kay in reference to determination of the item authenticity. This citation is unavailing as Kay describes that the authenticity of the item is based on a comparison, not between the numbers recited in claim 1, but between the information stored in a machine at the event and the number printed by the customer.

The Office Action now turns to Halperin for the numbers (which is confusing as the Office Action previously insists that the numbers are present in Kay) and the RFID tag. In Halperin the encryption of the serial number of the label is on the RFID tag while as recited in claim 1, a number is on the RFID tag (e.g., the serial number plus the unique number) and the signature of RFID contents is on the label. The numbers associated with the barcode and RFID tag in Halperin are duplicative, unlike that recited in claim 1. Moreover, the method of claim 1 recognizes a benefit over conventional RFID tags as the encrypted information contained in the conventional RFID tag in Halperin has a large number of bits. This is not desirable due to the limited memory in, and cost of, RFID tags. By separately providing the encrypted information on a label while providing the unencrypted information in the RFID tag, as recited in claim 1, these disadvantages can be overcome.

Claim 1 thus specifically recites the use of an RFID tag and printed label having specific information. Assuming one would have some reason to add the use of an RFID tag to that of printed label in the situations described by Kay, the combination of Halperin and Kay would

result in information contained in the RFID tag and printed label that is duplicative. This is to say that the combined method would have to be further altered as the information in the RFID tag of Halperin is encrypted, whereas as recited in claim 1 the information in the RFID tag is not signed. Moreover, the combination of Kay and Halperin would result in both being compared to the information stored in the portable terminal of Kay. This is not what is recited in claim 1, in which the information in the RFID tag and printed label are compared (after using a cryptographic process) rather than comparing one or both to another, separate number.

The Office Action asserts, however, that the RFID tag could be used to replace the memory device of Kay merely because they are both memory devices. In other words, the Office Action insists that the event officials would have access to hundreds or thousands of RFID tags containing the same information as on individual tickets (as it would be impossible to retain all of the information on a single RFID tag, let alone the problems involved in reading such a tag). Applicant respectfully requests that if the next Office Action continues to insist that a substitution of this type is viable, it explain why and how one of skill in the art would and could effect this substitution.

Ignoring all of the above, there is no reason why one of skill in the art would combine the teachings of Kay and Halperin to arrive at the method recited in claim 1. Kay describes the use of a customer printing his/her own ticket at home by his/her computer. It is unlikely, to say the least, that either the customer would use an RFID tag in addition to a printed ticket (let alone having the equipment necessary to program the RFID tag) or event officials would use RFID tags. It is also unlikely that an RFID tag could be used in a situation described by Kay – e.g., why would a customer (or a ticket taker at the event) use separate RFID tags, where would the RFID tags be located, how would the RFID tags be used? Applicant respectfully requests that if the next Office Action continues to insist that one of skill in the art would be motivated to combine Kay and Halperin, it furthermore explain why and how one of skill in the art would and could employ the RFID tags.

For at least these reasons, none of the references anticipate or disclose the method recited in claim 1. Thus, claim 1 is patentable over the cited references.

For at least similar reasons, none of the references anticipate or disclose the method recited in claims 6, 11 or 21. Thus, claims 6, 11 or 21 are patentable over the cited references.

In addition, claims 6 and 21 recites further specifics about the RFID tag. For example, claim 6 recites that the RFID tag contains two numbers: a first number that is unalterable and essentially unique and a separate second number that is programmed into the RFID tag having the first number. Similarly, claim 21 recites that the two numbers are obtained by radio means. Nowhere does Halperin disclose that the RFID tag is has two separate numbers or that the RFID tag programmed first with an unalterable number and then later programmed with another number. In other words, it is apparent that the number in Halperin is a single encrypted number that was programmed when the product was labeled. Moreover, Halperin nowhere teaches that one of these numbers is alterable and the other is unalterable as recited in the claims. Furthermore, Halperin nowhere teaches that the combination of these unalterable and alterable numbers is then signed and affixed as recited in the claims.

Claims 5, 8, 19-20 and 22-33 are dependent on an allowable base claim and thus themselves are allowable without more. These claims are also independently allowable. For example, claim 22 recites that the RFID tag is an anti-forgery RFID tag. It is clear through the doctrine of claim differentiation, and as recognized by the Office Action, that an anti-forgery RFID tag is a specific embodiment of a RFID tag. An anti-forgery RFID tag is defined in the paragraph beginning on page 3, line 22 of the instant application. Per MPEP 2111, such a definition must be used when employing the broadest reasonable interpretation of this claim. Nowhere is the anti-forgery RFID tag of claim 22 disclosed in Halperin. Other claims further differentiate the unalterable number with the other number by determining whether the second number is an EPC of the item, such as in claim 26 or that the first number does not contain product information of the item whereas the second number contains product information of the item. Claim 23 recites electronically determining whether a specific physical feature or a behavioral feature of the RFID tag matches that of an anti-forgery RFID tag. Nowhere does Halperin disclose this limitation – the paragraph cited by the Office Action describes a physical tamper detection mechanism of the product that has nothing to do with the RFID tag. The tamper proof seal of Halperin thus has nothing to do with matching either a physical or behavioral feature with that of an anti-forgery RFID tag, let alone doing so electronically.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case and such action is earnestly solicited. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's attorney or agent at the telephone number indicated below. Applicant herein petitions for any extension of time necessary for the filing of this response. Please charge any fees that may be due for this filing to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,

SEND CORRESPONDENCE TO:

Motorola, Inc.
1303 East Algonquin Road
IL01/3rd Floor
Schaumburg, IL 60196
Customer Number: 22917

By: /Anthony P. Curtis/

Anthony Curtis
Attorney of Record
Reg. No.: 46,193

Telephone:847-576-1974
Fax No.: 847-576-0721
Email: acurtis@motorola.com